THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants: Fetkovich et al.

Group Art Unit: 2171

Serial No.: 09/443,204

Examiner: Patrick J.D. Santos

Filed: 11/18/99

Appeal No.:

For: DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on January 27, 2005.

Kevin P. Radigan
Attorney for Appellants
Registration No. 31,789

Date of Signature: January 27, 2005

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Appellants' Reply Brief

Dear Sir:

This Reply Brief is filed pursuant to 37 C.F.R. §41.41 in rebuttal to certain characterizations and conclusions set forth in the Examiner's Answer mailed December 14, 2004, for the above-designated Appeal.

Remarks

Applicants respectfully traverse various characterizations and conclusions contained in paragraph 11, the Response to Arguments portion of the Examiner's Answer (at pages 36-44).

As noted in their Appeal Brief, Appellants respectfully submit that Jones in combination with Nardone and Leppek do not disclose their recited method for protecting a stream of data to be transferred between an encryption unit and a decryption unit which includes (in part) the process of dynamically varying the encrypting of the stream of data at the encryption unit by dynamically changing simultaneously multiple encryption parameters. At pages 37 & 38 of his Answer, the Examiner's position with respect to the three applied references is summarized, including the alleged insights drawn from each reference. Various ones of these insights are respectfully traversed to the extent deemed applicable to Appellants' above-noted process for dynamically changing the encryption process.

At page 37, the Examiner alleges that "The insight of Nardone '700 is the use of policies to specify parameters to vary and that the dynamic changing simultaneously multiple encryption parameters via dynamically changing policies." (emphasis added) Appellants respectfully submit that this insight mischaracterizes the teachings of Nardone.

Nardone describes a policy-based selective encryption of compressed video data. Basic transfer units (BTUs) of compressed video data of a video image are selectively encrypted in Nardone in accordance with an encryption policy to degrade the video image to at least a virtually useless state, i.e., if the selectively encrypted compressed video image were to be rendered without decryption. In Nardone, an encryption policy refers to the encryption duty cycle. As stated at column 1, lines 40-59 thereof, Nardone achieves degradation that approximates the level provided by a total encryption approach, but requiring only a fraction of the processor cycle cost of the total encryption approach by selectively encrypting certain basic transfer units. This selective encryption occurs in Nardone at authoring time; and at authoring time, which basic transfer units are to be encrypted may be dynamically adjusted. As explained by Nardone, in one embodiment, where the video images are MPEG compressed, all BTUs containing either the start code for a group of pictures or the start code for a particular frame are

encrypted, to prevent recovery of the video frames. In an alternate embodiment, a fraction of the BTUs of an I-frame, and a fraction of the BTUs of a P-frame are encrypted, again, to destroy data references by future frames. Thus, the goal of Nardone is to reduce the processor cycle cost required to entirely encrypt video data of video images. The dynamic adjustment of encryption policies in Nardone is taught to change which basic transfer units are to be encrypted (i.e., the duty cycle of the encryption process), and not the encryption process *per se*. This change in the amount of encryption being applied to the video data of the video images does not teach or suggest that multiple encryption parameters are changed between policies.

Thus, Nardone describes a change in encryption policies to effect the amount of partial encryption applied to video data of a video image in order to ensure sufficient degradation of the video image to a virtually useless state (i.e., if the selectively encrypted compressed video images were to be rendered without decryption), while requiring only a fraction of the processor cycle cost compared to a total encryption process. Because the policy selection at authoring time described by Nardone only presents a change in the duty cycle, i.e., a change in which basic transfer units of the video data are to be encrypted, Appellants respectfully submit that Nardone does not provide an insight as characterized in the Examiner's Answer. The only "parameter" being change with a dynamic adjustment in policy in Nardone is a change in the duty cycle of the encryption of the basic transfer units. The Examiner's Answer points to no teaching or suggestion in Nardone that a change in encryption policy from one fractual encryption to another fractual encryption equates to a simultaneous change in multiple encryption parameters. To characterize the teachings of Nardone otherwise is believed to result from a hindsight reference to Appellants' own invention. The Examiner notes at page 37 that "While varying the degree of selective encryption in order to degrade video images one possible encryption parameter to vary, it is not the only encryption parameter to vary." (emphasis added) However, no section of Nardone is cited for supporting the alleged insight that multiple encryption parameters can be simultaneously changed when dynamically changing policies.

In apparent conflict to the Examiner's above-cited insight with respect to Nardone, the Examiner's Answer acknowledges at the bottom of page 37 that Nardone is not explicit about setting multiple parameters in a policy. However, on page 38, the Examiner's Answer alleges

that the insight of Leppek is the application of multiple encryption operators at once. Again, Appellants respectfully submit that this insight is a hindsight mischaracterization of the teachings of Leppek, that is, to the extent deemed applicable to their claimed process.

Leppek describes a virtual encryption scheme which combines different encryption operators into a compound-encryption mechanism. The encryption "operators" in Leppek refer to different encryption "algorithms". For example, reference column 1, lines 54-56 where it is stated that a fundamental characteristic of essentially all encryption operators or algorithms is the fact that, given enough resources, almost any encryption algorithm can be broken. Thus, the encryption operators in Leppek are encryption algorithms and do not equate to Appellants' recited process wherein Appellants dynamically varying the encrypting of a stream of data by dynamically changing simultaneously multiple encryption parameters of the encrypting process.

In Leppek, data is first encoded using a first encryption operator (i.e., algorithm), then the same data is encoded using a second encryption operator, etc., thereby increasing the entropy of the data to make the encoded data look as random as possible. This approach is contrasted with Appellants' recited process wherein they dynamically change simultaneously multiple encryption parameters while an encryption unit is encrypting a stream of data. In Appellants' approach, different segments of the stream of data are encrypted using different encryption parameters and there is a dynamic change in the encryption parameters such that the multiple encryption parameters simultaneously change from one segment to another segment of the stream of data as the stream of data is passing through the encryption unit and being encrypted. In Leppek, there is a static, sequential application of a number of encryption algorithms (or encryption operators) to the same segment of data.

The Examiner's Answer seeks to equate Leppek's teaching of a compound sequence of encryption operators, i.e., the sequential application of encryption algorithms, to Appellants' recited language of simultaneously changing multiple encryption parameters during the dynamically varying of the encrypting of a stream of data. This conclusion is respectfully traversed. Leppek does not teach the application of multiple encryption operators being applied to the data simultaneously. Rather, Leppek describes a sequential application of encryption algorithms to the same data to increase the entropy of the data. For example, reference column

4, lines 58-67 where Leppek teaches a successive process of accessing sequentially differing encryption operators (i.e., algorithms) and wrapping the previously encrypted data until the last access code in the encryption control sequence is processed. Clearly, the sequential application of encryption operators (i.e., algorithms) to the same data does not equate to the alleged insight of the application of multiple encryption operators at once. First, the encryption operators described by Leppek are encryption algorithms, and do not equate to the encryption parameters recited in Appellants' encryption process. Secondly, there is no simultaneous application of multiple encryption operators (i.e., algorithms) in Leppek. Rather, Leppek expressly teaches the sequential application of encryption operators (i.e., algorithms) to the data so as to wrap the previously encrypted data with the next encryption operator algorithm.

For the above reasons, Appellants respectfully submit that the alleged insights drawn from Nardone and Leppek are a mischaracterization of the teachings of those patents, and therefore reconsideration and reversal of the obviousness rejection to their independent claims based upon Jones, Nardone and Leppek is requested.

Further, because Appellants' approach does not rely upon any predefined policy (such as in Jones), Appellants' process recites dynamically varying the encrypting of a stream of data at the encryption unit by dynamically changing simultaneously multiple encryption parameters and signaling the dynamic change in encryption parameters to the decryption unit. Since the dynamic varying of the encrypting of the stream of data occurs at the encryption unit, the encryption unit signals the dynamic change to the decryption unit. Jones, Nardone and Leppek do not describe any mechanism for signaling dynamic changes in multiple parameters from an encryption unit to a decryption unit. In this regard, the Examiner's Answer references at page 39, paragraph 12 of the final Office Action, where it is alleged that Jones requires the exchange of random number seed values and interval values between the encryptor and the decryptor. (Jones, column 1, line 66 – column 2, line 7). This characterization of the teachings of Jones is respectfully traversed. In Jones, a seed value and interval value are established *a priori*, before an encryption process begins and are provided as inputs to both the encryption unit and the decryption unit as shown in FIG. 1 of Jones. Since they are provided *a priori* as inputs to both units, there is no signaling from the encryption unit to the decryption unit of the simultaneous

change of multiple encryption parameters. For this additional reason, Appellants allege error in rejecting their independent claims as obvious over the combination of Jones, Nardone and Leppek.

In evaluating claimed subject matter as a whole, the Federal Circuit has mandated that functional claim language be considered in evaluating a claim relative to the prior art. Appellants respectfully submit that the application of this standard to their independent claims leads to the conclusion that the recited subject matter would not have been obvious to one of ordinary skill in the art based on the teachings of Jones, Nardone and Leppek.

For at least the above-stated reasons, as well as for those set forth in the Appeal Brief, Appellants respectfully request reversal of all rejections.

Respectfully submitted,

Kevin P. Radigan

Kevin P. Radigan
Reg. No. 31,789
Attorney for Appellants

Dated: January 27, 2005

HESLIN ROTHENBERG FARLEY & MESITI, P.C.
5 Columbia Circle
Albany, New York 12203
Telephone: (518) 452-5600
Facsimile: (518) 452-5579

TRANSMITTAL LETTER (General - Patent Pending)	Docket No. EN998146

In Re Application Of: **Fetkovich et al.**

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
09/443,204	11/18/1999	Patrick J.D. Santos	46369	2171	6903

Title: **DYNAMIC ENCRYPTION AND DECRYPTION OF A STREAM OF DATA**

COMMISSIONER FOR PATENTS:

Transmitted herewith is:

* **Appellants' Reply Brief (6 pgs.); and**
* **Return Receipt Postcard.**

in the above identified application.

- ☒ No additional fee is required.
- ☐ A check in the amount of is attached.
- ☒ The Director is hereby authorized to charge and credit Deposit Account No. **09-0457 (IBM)** as described below.
  - ☐ Charge the amount of
  - ☒ Credit any overpayment.
  - ☒ Charge any additional fee required.
- ☐ Payment by credit card. Form PTO-2038 is attached.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Kevin P. Radigan
Signature

Dated: **January 27, 2005**

Kevin P. Radigan, Esq.
Registration No.: 31,789

HESLIN ROTHENBERG FARLEY & MESITI, P.C.
5 Columbia Circle
Albany, New York 12203
Tel: (518) 452-5600
Fax: (518) 452-5579

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on **January 27, 2005**
(Date)

Kevin P. Radigan
Signature of Person Mailing Correspondence

Kevin P. Radigan
Typed or Printed Name of Person Mailing Correspondence

cc: